Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Modernizing the E-Rate Program for Schools and Libraries	)	WC Docket No. 13-184
	)	
	)	
Wireline Competition Bureau Seeks Comment On Proposed Eligible Services List for The E-Rate Program	)	
	)	
	)	

COMMENTS OF COX COMMUNICATIONS, INC.

Cox Communications, Inc., ("Cox") hereby submits these comments in response to the Wireline Competition Bureau's ("Bureau") public notice regarding the proposed Eligible Services List ("ESL") for funding year 2017.[1] Cox urges the Bureau to include Distributed Denial of Service ("DDoS") attack prevention and mitigation services on the ESL for funding year 2017. Although the Commission declined to include E-Rate support for "further network security services," such as DDoS attack prevention and mitigation services, in the 2014 Modernization Order,[2] it did so without significant deliberation or a robust record. Since that time, based on informal feedback from our educational customers and online news sources, schools across the country have experienced a marked increase in the number of DDoS attacks,[3] which warrants a fresh look at this network security service.

A DDoS attack is an attempt from an outside individual or group to overload network systems, equipment and memory resources. DDoS attacks are unique from other types of malware or viruses, because they do not simply slow down Internet service; they can cripple

---

[1] Wireline Competition Bureau Seeks Comment on Proposed Eligible Services List for the E-Rate Program, DA 16-615 (Enf. Bur. rel. June 3, 2016).

[2] *See Modernizing the E-Rate Program for Schools and Libraries,* Report and Order and Further Notice of Proposed Rulemaking, 29 FCC Rcd 8870, 8918, para 121 & n. 275 ("*Modernization Order*") (declining to designate services suggested by commenters, including intrusion protection and detection, malware protection, application control, content filters, DDoS mitigation, and cybersecurity services, as eligible in three sentences).

[3] *See, e.g.,* "What Happens When Student Hackers Shut Down a District's Internet," e School News at http://www.eschoolnews.com/2016/03/16/what-happens-when-student-hackers-shut-down-a-districts-internet/; "Salt Lake Schools Hit With DDoS Attack," SC Magazine at http://www.scmagazine.com/salt-lake-schools-hit-with-ddos-attack/article/451480/; "Teen Pays for DDoS on School" at http://www.geek.com/news/teen-pays-for-ddos-on-school-faces-felony-charges-1623599/; "Michigan High School Student Facing Charges After Launching DDoS Attack on School Network" at https://www.ddosattacks.net/michigan-high-school-student-facing-charges-after-lauching-ddos-attack-on-school-network/.

systems and effectively result in a temporary loss of Internet service. In addition, certain types of reflective DDoS attacks[4] can saturate Internet broadband circuits, leaving local firewall appliances helpless to restrict unwanted traffic. Available DDoS services include monitoring school and library networks for DDoS attacks and mitigation of attacks by filtering out unwanted traffic.

Because DDoS attacks can render Internet service effectively unusable, support for DDoS services are necessary to protect the E-Rate fund's investment in Internet access and the integrity of educational networks. The Commission's first goal is modernizing the E-rate program was "ensuring affordable access to high-speed broadband sufficient to support digital learning in schools and robust connectivity for all libraries."[5] Inclusion of DDoS attack prevention and mitigation services will further this goal by ensuring that schools and libraries continue to have access to the high-speed services made possible by the E-rate program.

The increase in DDoS attacks against school networks anecdotally appears to be related to increases in the use of online standardized testing.[6] Instead of calling in sick, some students have allegedly used DDoS attacks to delay taking online standardized tests. As more schools utilize online testing, it would not be surprising to see an even larger increase in DDoS attacks. Given that educators have incorporated the Internet into all aspects of the classroom experience – from storing lesson plans on cloud servers, to contacting parents through email and blogs, to accessing online educational materials – the loss of Internet access during standardized testing days is particularly acute. Making E-Rate support available for DDoS services will better enable schools to protect their networks and prevent DDoS attacks from negatively impacting classroom learning and testing, the conduct of school business, and communication with students, parents, and extended communities.

---

[4] A reflective attack may involve sending forged requests to a large number of computers that will reply to the requests and send those replies to the targeted victim through the use of Internet Protocol address spoofing.
[5] *Modernization Order*, 29 FCC Rcd at 8881, para. 26.
[6] *See* "Florida Testing Troubles Caused by Cyber Attack" at http://www.miamiherald.com/news/local/education/article13121993.html.

Based on the reasons outlined herein, Cox respectfully requests that the Bureau include DDoS attack prevention and mitigation services on the ESL for funding year 2017.

Respectfully submitted.

By: Joiava Philpott

Joiava Philpott
Vice President, Regulatory Affairs
Cox Communications, Inc.
6205 Peachtree Dunwoody Road
Atlanta, GA 30328

July 5, 2016